Induction: Proving “For All...”
Reading

  - Chapter 5
Overview: Induction, Proving “…for all…”

• What is induction
• Why do we need it?
• The principle of induction
  – Toppling the dominos
  – The induction template
• Examples
• Induction, Well-Ordering and the Smallest Counter-Example
Dispensing postage using 5¢ and 7¢ stamps

• How do I pay for a 19¢ letter?
  – using 7,7,5 stamps

• How about 20?
  – using 5,5,5,5 stamps

• How about 21?
  – using 7,7,7 stamps

• How about 22?
  – using 5,5,5,7 stamps

• How about 23?
  – ?
  – Looks hard
Dispensing postage using 5¢ and 7¢ stamps

• How do I pay for a 19¢ letter?
  – using 7,7,5 stamps
  – What about 24?
    • 7,7,5,5
• How about 22?
  – using 5,5,5,7 stamps
  – What about 27?
    • 5,5,5,7,5
• Can every postage greater than 23¢ can be dispensed?
  – Intuitively, yes
  – Induction formalizes this intuition
Why do we need induction?

• Predicate: \( P(n) = \text{“5¢ and 7¢ stamps can make postage } n.\text{”} \)
  – Claim: \( \forall n \geq 24: P(n) \)
  – Seems true

• Predicate: \( P(n) = \text{“} n^2 - n + 41 \text{ a prime number.”} \)
  – Claim: \( \forall n \geq 1: P(n) \)
  – Try different \( n \)
    • \( n = 1: 41 \text{ (prime)} \)
    • \( n = 2: 43 \text{ (prime)} \)
    • \( n = 3: 47 \text{ (prime)} \)
    • \( n = 4: 53 \text{ (prime)} \)
    • ... 
    • \( n = 41: 1681 \text{ (not prime!)} \)
Why do we need induction?, cont’d

• Predicate: \( P(n) = \text{“}4n - 1 \text{ is divisible by 3.”} \)
  
  – Claim: \( \forall n \geq 1: P(n) \)
  
  – Try different \( n \)
    
    • \( n = 1 \rightarrow 4 - 1 = 3 \) (yes)
    
    • \( n = 2 \rightarrow 8 - 1 = 7 \) (nope)

• How can we prove something for \textit{all} \( n \geq 1 \)? Checking each \( n \) takes too long!

• Prove for general \( n \). Can be tricky.

• \textbf{Induction}. Systematic.
Is $4^n - 1$ divisible by 3 for $n \geq 1$?

- Predicate: $P(n) = "4^n - 1$ is divisible by 3."
- We proved
  - IF $4^n - 1$ is divisible by 3, THEN $4^{n+1} - 1$ is divisible by 3

- **Theorem:** Let $x$ be any real number, i.e., $x \in \mathbb{R}$. IF $4^x - 1$ is divisible by 3, THEN $4^{x+1} - 1$ is divisible by 3.
- **Proof:** We prove the claim using a direct proof.
  1. Assume that $p$ is T, that is $4^x - 1$ is divisible by 3.
  2. This means that $4^x - 1 = 3k$ for an integer $k$, or that $4^x = 3k + 1$
  3. Observe that $4^{x+1} = 4 \times 4^x$. Using $4^x = 3k + 1$,
     note that $4^{x+1} = 4(3k + 1) = 12k + 4$
  4. Therefore $4^{x+1} - 1 = 12k + 3 = 3(4k + 1)$ is a multiple of 3 (4$k + 1$ is an integer)
  5. Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3
  6. Therefore, the statement claimed in $q$ is T
Is $4^n - 1$ divisible by 3 for $n \geq 1$?

- Predicate: $P(n) = "4^n - 1 is divisible by 3."$
- We proved
  - IF $4^n - 1$ is divisible by 3, THEN $4^{n+1} - 1$ is divisible by 3
  - So we proved: IF $P(n)$ THEN $P(n + 1)$
  - i.e., $P(n) \rightarrow P(n + 1)$
- What use is this?
  - (Reasoning in the absence of facts.)
Is $4^n - 1$ divisible by 3 for $n \geq 1$?

• We proved
  – IF $4^n - 1$ is divisible by 3, THEN $4^{n+1} - 1$ is divisible by 3
  – So we proved IF $P(n)$ THEN $P(n + 1)$
  – i.e., $P(n) \rightarrow P(n + 1)$

• From tinkering, we know
  
  $P(1)$ is T: $4^1 - 1 = 3$ is divisible by 3

• $P(1) \rightarrow P(2)$
• $P(2) \rightarrow P(3)$
• $P(3) \rightarrow P(4)$
• $P(4) \rightarrow P(5)$

• When does this end??
Is $4^n - 1$ divisible by 3 for $n \geq 1$?

- We know $P(1)$ is T
  
  $$4^1 - 1 = 3$$ is divisible by 3

- We also know $P(n) \rightarrow P(n + 1)$

- By induction, $P(n)$ is T for all $n \geq 1$

- $P(n)$ form an infinite chain of dominos

- Topple the first and they *all* fall

- **Practice**: Exercise 5.2
Induction Template

- **Induction to prove**: \( \forall n \geq 1: P(n) \)
- **Proof**. We use induction to prove: \( \forall n \geq 1: P(n) \)
  1. Show that \( P(1) \) is T ("simple" verification) [**base case**]
  2. Show \( P(n) \rightarrow P(n + 1) \) for \( n \geq 1 \) [**induction step**]
    - Use **Direct** proof
    - Assume \( P(n) \) is T
      - (valid derivations)
      - must show for any \( n \geq 1 \)
      - must use \( P(n) \) here
    - Show \( P(n + 1) \) is T
• **Induction to prove**: $\forall n \geq 1: P(n)$

• **Proof.** We use induction to prove: $\forall n \geq 1: P(n)$
  1. Show that $P(1)$ is T ("simple" verification) **[base case]**
  2. Show $P(n) \rightarrow P(n + 1)$ for $n \geq 1$ **[induction step]**
     - Use Proof by **Contraposition**
     - Assume $P(n + 1)$ is F
       - (valid derivations)
       - must show for any $n \geq 1$
       - must use $\neg P(n + 1)$ here
     - Show $P(n)$ is F
Induction Template

- **Induction to prove:** \( \forall n \geq 1: P(n) \)

Proof. We use induction to prove: \( \forall n \geq 1: P(n) \)

1. Show that \( P(1) \) is T ("simple" verification) [**base case**]
2. Show \( P(n) \rightarrow P(n + 1) \) for \( n \geq 1 \) [**induction step**]
   - Use **Direct proof**
   - Assume \( P(n) \) is T
     - (valid derivations)
     - must show for any \( n \geq 1 \)
     - must use \( P(n) \) here
   - Show \( P(n + 1) \) is T
   - Use Proof by **Contraposition**
   - Assume \( P(n + 1) \) is F
     - (valid derivations)
     - must show for any \( n \geq 1 \)
     - must use \( \neg P(n + 1) \) here
   - Show \( P(n) \) is F
3. Conclude: by induction: \( \forall n \geq 1: P(n) \)
Induction Template, cont’d

• Prove the implication $P(n) \rightarrow P(n + 1)$ for a general $n \geq 1$
• Why is this easier than just proving $P(n)$ for general $n$?
  – Assuming $P(n)$ is T gives us a lot of information to work with
• Assume $P(n)$ is T, and reformulate it mathematically
• Somewhere in the proof you must use $P(n)$ to prove $P(n + 1)$
• End with a statement that $P(n + 1)$ is T
Sum of Integers

• What is the sum $1 + 2 + 3 + \cdots + (n - 1) + n$
  – Can you give an expression as a function of $n$?

• The mathematician Gauss was one day sitting in class and was bored, so his teacher asked him to calculate $1 + 2 + \cdots + 100$
  – he started playing around with numbers:
    \[
    S(n) = 1 + 2 + \cdots + n \\
    S(n) = n + n - 1 + \cdots + 1
    \]

• So, $2S(n) = (n + 1) + (n + 1) + \cdots + (n + 1)$
  – i.e., $2S(n) = n \times (n + 1)$
  – i.e., $S(n) = \frac{n(n+1)}{2}$

• This is direct proof!
  – Note that this proof technique requires ingenuity in general
Proof by induction: $\sum_{i=1}^{n} i = \frac{1}{2} n(n + 1)$

- **Proof**: (By induction) $P(n): \sum_{i=1}^{n} i = \frac{1}{2} n(n + 1)$

1.  **[Base Case]** $P(1)$ claims that $1 = \frac{1}{2} \times 1 \times (1 + 1)$
   - Clearly T

2.  **[Induction Step]** We show $P(n) \rightarrow P(n + 1)$ for all $n \geq 1$, using direct proof.
   - Assume (induction hypothesis) $P(n)$ is T: $\sum_{i=1}^{n} i = \frac{1}{2} n(n + 1)$
   - Need to show $P(n + 1)$ is T: $\sum_{i=1}^{n+1} i = \frac{1}{2} (n + 1)(n + 1 + 1)$
     \[
     \sum_{i=1}^{n+1} i = \left( \sum_{i=1}^{n} i \right) + (n + 1) \tag{key step}
     \]
     \[
     = \frac{1}{2} n(n + 1) + (n + 1) \tag{induction hypothesis $P(n)$}
     \]
     \[
     = (n + 1) \left( \frac{1}{2} n + 1 \right) = \frac{1}{2} (n + 1)(n + 2) \tag{algebra}
     \]
     \[
     = \frac{1}{2} (n + 1)(n + 2) \tag{what needed to be shown}
     \]

3.  By induction, $P(n)$ is T for all $n \geq 1$
BEWARE of going in the wrong direction!

• If we had started from \( n + 1 \)

\[
\sum_{i=1}^{n+1} i = \frac{1}{2} (n + 1)(n + 2)
\]

– This is what we would like to show

• It follows that:

\[
\sum_{i=1}^{n+1} i - (n + 1) = \frac{1}{2} (n + 1)(n + 2) - (n + 1)
\]

\[
\sum_{i=1}^{n} i = (n + 1) \left( \frac{1}{2} n + 1 - 1 \right) = \frac{1}{2} n(n + 1)
\]

Hooray!

Or is it...
**BEWARE of going in the wrong direction!**

- Suppose we assume $7 = 4$
- This means that $4 = 7$
  - because $(a = b) \rightarrow (b = a)$
- If we add both equations, we get $11 = 11$
  - Just because the final result makes sense doesn’t mean that we did something right
  - By assuming $4 = 7$, we proved that $11 = 11$
  - But did we actually prove $4 = 7$?
- To start, you can **NEVER** assert (as though it’s true) what you are trying to prove
Sum of Integer Squares

- What is the sum $1^2 + 2^2 + 3^2 + \cdots + (n - 1)^2 + n^2$?
  - Need to channel our inner Gauss
  - Unfortunately, he didn’t solve this one
    - Or didn’t think it was important enough to write down...
- Let’s play around with some numbers first
  \[
  S(1) = 1 \\
  S(2) = 5 \\
  S(3) = 14 \\
  S(4) = 30 \\
  S(5) = 55 \\
  S(6) = 91 \\
  S(7) = 140
  \]
Sum of Integer Squares, cont’d

• Let’s play around with some numbers first
  \[ S(1) = 1, S(2) = 5, S(3) = 14, S(4) = 30, S(5) = 55, S(6) = 91, S(7) = 140 \]

• How about \( S'(n) = S(n + 1) - S(n) \)?
  – All the squares: 4, 9, 16, 25, 36, 49

• How about \( S''(n) = S'(n + 1) - S'(n) \)?
  – All odd numbers: 5, 7, 9, 11, 13

• How about \( S'''(n) = S''(n + 1) - S''(n) \)?
  – Constant: 2, 2, 2, 2

• Hm... Difference is kind of like a derivative
  – If a function’s 4\(^\text{th}\) derivative is 0, then we know the function is a 3\(^\text{rd}\) order polynomial
  – Perhaps we can approximate \( S(n) \) in a Taylor-series-like way and see if that works
Sum of Integer Squares, cont’d

- Recall Taylor series expansion (around point $x_0$):

$$\hat{f}(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{1}{2}f''(x_0)(x - x_0)^2 + \frac{1}{6}f'''(x_0)(x - x_0)^3$$

  - Higher-order terms are 0 if third derivative is constant

- “Taylor series” guess

$$S(n) = a_0 + a_1 n + a_2 n^2 + a_3 n^3$$

- Let’s plug in a few values for $n$ and see if can solve for the $a$’s

  $S(1) = 1 = a_0 + a_1 + a_2 + a_3$
  $S(2) = 5 = a_0 + 2a_1 + 4a_2 + 8a_3$
  $S(3) = 14 = a_0 + 3a_1 + 9a_2 + 27a_3$
  $S(4) = 30 = a_0 + 4a_1 + 16a_2 + 64a_3$

  - How do we solve a linear system of equations?
  - Gaussian elimination! (thank you, Gauss, after all)
• “Taylor series” guess

\[ S(n) = a_0 + a_1 n + a_2 n^2 + a_3 n^3 \]

• Let’s plug in a few values for \( n \) and see if can solve for the \( a \)’s

\[
\begin{align*}
S(1) &= 1 = a_0 + a_1 + a_2 + a_3 \\
S(2) &= 5 = a_0 + 2a_1 + 4a_2 + 8a_3 \\
S(3) &= 14 = a_0 + 3a_1 + 9a_2 + 27a_3 \\
S(4) &= 30 = a_0 + 4a_1 + 16a_2 + 64a_3 \\
\end{align*}
\]

• Solution is \( a_0 = 0, a_1 = \frac{1}{6}, a_2 = \frac{1}{2}, a_3 = \frac{1}{3} \)

  - Solve for \( a_0 \) in terms of other \( a \)’s; then solve for \( a_1 \), etc.

• So guess is \( S(n) = \frac{1}{6} n + \frac{1}{2} n^2 + \frac{1}{3} n^3 \)

  - \( S(1) = 1, S(2) = 5, S(3) = 14, ... \)

  - Hm, seems correct. Let’s prove it using induction!
Proof: $S(n) = \sum_{i=1}^{n} i^2 = \frac{1}{6} n + \frac{1}{2} n^2 + \frac{1}{3} n^3$

- **Proof:** (By induction)

  \[ P(n): \sum_{i=1}^{n} i^2 = \frac{1}{6} n + \frac{1}{2} n^2 + \frac{1}{3} n^3 = \frac{1}{6} n(n + 1)(2n + 1) \]

1. **[Base case]** $P(1)$ claims that $1 = \frac{1}{6} \times 1 \times 2 \times 3$, which is T

2. **[Induction step]** Show $P(n) \rightarrow P(n + 1)$ for all $n \geq 1$. Direct proof.
   - Need to show $P(n + 1)$ is T:
     \[ \sum_{i=1}^{n+1} i^2 = \frac{1}{6} (n + 1)(n + 2)(2n + 3) \]
     \[ \sum_{i=1}^{n+1} i^2 = (\sum_{i=1}^{n} i^2) + (n + 1)^2 \quad \text{[key step]} \]
     \[ = \frac{1}{6} n(n + 1)(2n + 1) + (n + 1)^2 \quad \text{[induction hypothesis $P(n)$]} \]
     \[ = \frac{1}{6} (n + 1)(2n^2 + 7n + 6) \quad \text{[algebra]} \]
     \[ = \frac{1}{6} (n + 1)(2n^2 + 4n + 3n + 6) \quad \text{[algebra]} \]
     \[ = \frac{1}{6} (n + 1)(n + 2)(2n + 3) \quad \text{[what needed to be shown]} \]
Proof: \( S(n) = \sum_{i=1}^{n} i^2 = \frac{1}{6} n + \frac{1}{2} n^2 + \frac{1}{3} n^3 \)

- **Proof:** (By induction)

  \[
P(n): \sum_{i=1}^{n} i^2 = \frac{1}{6} n + \frac{1}{2} n^2 + \frac{1}{3} n^3 = \frac{1}{6} n(n+1)(2n+1)
  \]

1. **[Base case]** \( P(1) \) claims that \( 1 = \frac{1}{6} \times 1 \times 2 \times 3 \), which is T

2. **[Induction step]** Show \( P(n) \rightarrow P(n + 1) \) for all \( n \geq 1 \). Direct proof.
   - Need to show \( P(n + 1) \) is T:
     \[
     \sum_{i=1}^{n+1} i^2 = \frac{1}{6} (n + 1)(n + 2)(2n + 3)
     \]
     \[
     \sum_{i=1}^{n+1} i^2 = \frac{1}{6} (n + 1)(2n^2 + 4n + 3n + 6) \quad \text{[algebra]}
     \]
     \[
     = \frac{1}{6} (n + 1)(n + 2)(2n + 3) \quad \text{[what needed to be shown]}
     \]
   - So \( P(n + 1) \) is T

- By induction, \( P(n) \) is T for all \( n \geq 1 \)
• Suppose we proved $P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow P(4) \rightarrow \cdots$

• What is missing?
  – **No base case!**

• Remember, $F \rightarrow T$!

• Suppose we want to prove:

$$P(n): n \geq n + 1 \text{ for all } n \geq 1$$

  – Add 1 to both sides:

$$n \geq n + 1 \rightarrow n + 1 \geq n + 2$$

  – Therefore, $P(n) \rightarrow P(n + 1)$

• [Every link is proved, but without the base case, you have *nothing*.]
  – **Broken chain!**
Induction gone wrong, cont’d

• False: $P(n)$: “all balls in any set of $n$ balls are the same color.”
  – **Base case.** $P(1)$ is T because there is only 1 ball
  – **Induction step.** Suppose any set of $n$ balls have the same color.
    • Consider any set of $n + 1$ balls $b_1, b_2, ..., b_n, b_{n+1}$.
    • So, $b_1, b_2, ..., b_n$ have the same color and $b_2, ..., b_n, b_{n+1}$ have the same color.
    • Thus $b_1, b_2, ..., b_n, b_{n+1}$ have the same color.
  – Does that mean $P(n) \rightarrow P(n + 1)$ for all $n \geq 1$?
    • Well, $P(1) \rightarrow P(2)$ is F
  • [A single broken link kills the entire proof.]

• How would you “fix” this proof?
  – Need two base cases!
  – Of course, now we can’t prove $P(2)$!
  – Phew, what a relief – the world is colorful after all!
• Recall the **Well-ordering Principle**:  
  – *Any* non-empty set of natural numbers has a minimum element.

• Induction follows from well ordering  
  – Let $P(1)$ and $P(n) \rightarrow P(n + 1)$ be T

• Suppose $P(n_*)$ fails for the **smallest** counter-example $n_*$ (well-ordering).  
  \[ P(1) \rightarrow P(2) \rightarrow P(3) \rightarrow \cdots \rightarrow P(n_* - 1) \rightarrow P(n_*) \rightarrow \cdots \]  
  – Now how can $P(n_* - 1) \rightarrow P(n_*)$ be T?

• **Any induction proof can also be done using well-ordering.**
Example Well-ordering Proof: $n < 2^n$ for all $n \geq 1$

- First prove it with induction
- Proof: [Induction] $P(n): n < 2^n$
  1. **[Base case]** $P(1)$ claims that $1 < 2^1$, which is T
  2. **[Induction step]** Assume $P(n)$ is T: $n < 2^n$
     - Need to show $P(n + 1)$ is T:
       $$n + 1 < 2^{n+1}$$
     - From the induction hypothesis:
       $$n + 1 \leq n + n \leq 2^n + 2^n = 2 \times 2^n = 2^{n+1}$$
Example Well-ordering Proof: $n < 2^n$ for all $n \geq 1$

- **Proof:** [Well-ordering] Proof by *contradiction*.
  - Assume that there is an $n \geq 1$ for which $n \geq 2^n$
  - Let $n_* \geq 1$ be the *minimum* such counter-example, $n_* \geq 2^{n_*}$
    - Using the well ordering axiom
      - Since $1 < 2^1$, then $n_* \geq 2$
      - Since $n_* \geq 2, \frac{1}{2} n_* \geq 1$ and so,
        \[
        n_* - 1 \geq n_* - \frac{1}{2} n_* = \frac{1}{2} n_* \\
        \geq \frac{1}{2} \times 2^{n_*} = 2^{n_*-1}
        \]
  - So, $n_* - 1$ is a *smaller* counter example. **FISHY!**
  - The *method of minimum counter-example* is very powerful.
Getting Good at Induction

• TINKER, TINKER, TINKER
• PRACTICE, PRACTICE, PRACTICE
• Just because something is not immediately obvious doesn’t mean you should give up
• **Challenge.** A circle has $2n$ distinct points, $n$ are red and $n$ are blue.
  – Prove that for all $n \geq 1$, there exists a blue point such that one can start at that blue point and move clockwise always having passed as many blue points as red.

• **Practice.** All exercises and pop-quizzes in chapter 5.
• **Strengthen.** Problems in chapter 5.